DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Eustace P. Isidore on 05/07/2009.

The application has been amended as follows:

Amend claims 1, 3-4, 10-11, 13-14, 20-21, 23-24 and 30.

Cancel claims 2, 12 and 22.

Claim 1:

(currently amended) A method of operating a communication network, comprising:

autonomously monitoring communication traffic at a communication port for an anomalous traffic;

detecting an anomaly in communication traffic at a plurality of nodes in the communication network, wherein the anomaly is an attack other than a worm or virus;

independently applying, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; ~~and~~

independently determining, at the respective ones of the plurality of nodes, a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B [[to]] stops the anomalous traffic; [[.]]

applying a logical combination of A and the second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B); and enforcing the logical combination (A & !B), if the logical combination (A & !B) stops the anomalous traffic.

Claim 2:

(cancelled)

Claim 3:

(currently amended) The method of claim [[2]] 1, further comprising: independently determining a third blocking measure C, at the respective ones of the plurality of nodes, such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & !B) stops the anomalous traffic.

Claim 4:

(currently amended) The method of claim [[2]] 1, wherein independently determining the second blocking measure B further comprises: applying a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic; and enforcing the logical combination (A & B), if the logical combination (A & B) stops the anomalous traffic.

Claim 10:

(currently amended) A method of operating a communication network, comprising:

detecting an anomaly in communication traffic at a plurality of nodes in the communication network;

synchronously applying, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; ~~and~~ synchronously determining, at the respective ones of the plurality of nodes, a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B [[to]] stops the anomalous traffic; [[.]]

applying a logical combination of A and the second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B); and enforcing the logical combination (A & !B), if the logical combination (A & !B) stops the anomalous traffic.

Claim 11:

(currently amended) A system for operating a communication network, comprising:

a processor;

program means executing on the processor including:

means for autonomously monitoring communication traffic at a communication port for an anomalous traffic;

means for detecting an anomaly in communication traffic at a plurality of nodes in the communication network, wherein the anomaly is an attack other than a worm or virus;

means for independently applying, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; ~~and~~

means for independently determining, at the respective ones of the plurality of nodes a, second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B [[to]] stop<u>s</u> the anomalous traffic<u>;</u> [[.]]

<u>means for applying a logical combination of A and the second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B); and means for enforcing the logical combination (A & !B), if the logical combination (A & !B) stops the anomalous traffic.</u>

Claim 12:

(cancelled)

Claim 13:

(currently amended) The system of claim [[12]] 11, further comprising:

means for independently determining, at the respective ones of the plurality of nodes, a third blocking measure C such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic, if the logical combination (A & !B) stops the anomalous traffic.

Claim 14:

(currently amended) The system of claim [[12]] 11, wherein the means for independently determining the second blocking measure B further comprises:

means for applying a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic; and

means for enforcing the logical combination (A & B), if the logical combination (A & B) stops the anomalous traffic.

Claim 20:

(currently amended) A system for operating a communication network, comprising:

means for detecting an anomaly in communication traffic at a plurality of nodes in the communication network;

means for synchronously applying, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; ~~and~~

means for synchronously determining a second blocking measure B at the respective ones of the plurality of nodes such that application of a logical combination of the first blocking measure A and the second blocking measure B [[to]] stops the anomalous traffic; [[.]]

means for applying a logical combination of A and the second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B); and means for enforcing the logical combination (A & !B), if the logical combination (A & !B) stops the anomalous traffic.

Claim 21:

(currently amended) A computer program product for operating a communication network, comprising:

a tangible computer storage medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code configured to autonomously monitor communication traffic at a communication port for an anomalous traffic;

computer readable program code configured to detect an anomaly in communication traffic at a plurality of nodes in the communication network, wherein the anomaly is an attack other than a worm or virus;

computer readable program code configured to independently apply, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; ~~and~~

computer readable program code configured to independently determine at the respective ones of the plurality of nodes a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B [[to]] stops the anomalous traffic; [[.]]

computer readable program code configured to apply a logical combination of A and the second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B); and computer readable program code configured to enforce the logical combination (A & !B), if the logical combination (A & !B) stops the anomalous traffic.

Claim 22:

(cancelled)

Claim 23:

(currently amended) The computer program product of claim 21 [[22]], further comprising:

computer readable program code configured to independently determine, at the respective ones of the plurality of nodes, a third blocking measure C such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & !B) stops the anomalous traffic.

Claim 24:

(currently amended) The computer program product of claim 21 [[22]], wherein the computer readable program code configured to independently determine the second blocking measure B further comprises:

computer readable program code configured to apply a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic; and

computer readable program code configured to enforce the logical combination (A & B), if the logical combination (A & B) stops the anomalous traffic.

Claim 30:

(currently amended) A computer program product for operating a communication network, comprising:

a tangible computer storage medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code configured to detect an anomaly in communication traffic at a plurality of nodes in the communication network;

computer readable program code configured to synchronously apply, at respective ones of the plurality of nodes, a first blocking measure A to the anomalous traffic that stops the anomalous traffic; ~~and~~

computer readable program code configured to synchronously determine at the respective ones of the plurality of nodes a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B [[to]] stops the anomalous traffic; [[.]]

computer readable program code configured to apply a logical combination of A and the second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B); and computer readable program code configured to enforce the logical combination (A & !B), if the logical combination (A & !B) stops the anomalous traffic.

Allowable Subject Matter

2. Claims 1, 3-11, 13-21 and 23-30 are allowed.

3. The following is an examiner's statement of reasons for allowance:

4. The present invention is directed to a method for monitoring at a communication port for an anomalous traffic. Each independent claim provide the distinct features of using a combination of the two blocking measures (i.e., a logical combination of A and the second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a less restrictive blocking measure than a logical combination (A & B)) to only block anomalous traffic at specific nodes, while allowing valid traffic to pass through. The closest prior arts fail to anticipate or render the above limitations obvious.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Trang Doan/
Examiner, Art Unit 2431

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2431